# Operational Security (OPSEC)

## Topics

Lesson 1 – Operational Security (OPSEC)

- Definition, process, and laws
- How OPSEC is used
- Persona and footprints
- Computer security
- Guidelines
- Summary



## Operational Security

- **Purpose**
  Define and provide the relevance of Operational Security
- **Objective**
  Students will use operational security in day-to-day operations, in both personal and professional lives

# Lesson 1

## Operational Security



## Definition

"Operations security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information."

Source: Joint Publications JP 3-13.3, Operations Security

LESSON 1



## Methodology

- Denies critical information to an adversary
- OPSEC measures identify, control, and protect generally unclassified evidence that is associated with sensitive operations and activities

Source: Joint Publications JP 3-13.3, Operations Security

LESSON 1

## The OPSEC Process

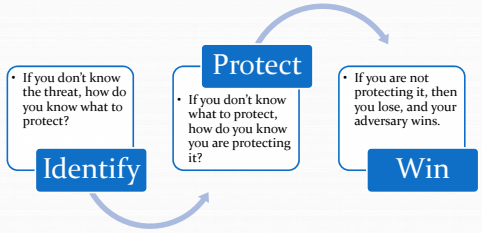
| | |
|---|---|
| Identify Critical Information | • Critical Information: information that would harm the organization's ability to effectively carry out normal operation if obtained by an adversary |
| Analyze the Threat | • Determine the individuals or groups that represent a threat to that information<br>• Capabilities, use for the information, determination, and resources must also be analyzed |
| Analyze the Vulnerabilities | • Thoroughly explore the vulnerabilities of the organization – physical safeguards, network/electronic safeguards, personnel training |
| Assess the Risks | • For each vulnerability, a threat is matched, and a risk level is assigned |
| Apply the Countermeasures | • Develop a plan to lower or eliminate the risk, or remove the threat's access to the resource<br>• Begin with the highest-risk vulnerabilities |

LESSON 1

8/17/2012 7

## OPSEC Laws

1. If you don't know the threat, how do you know what to protect?
2. If you don't know what to protect, how do you know you are protecting it?
3. If you are not protecting it, then you lose, and your adversary wins.




LESSON 1

8/17/2012 8

## OPSEC and OSINT

- "OSINT could unintentionally provide indicators of US military operations.
- Information generally available to the public as well as certain detectable activities such as **open source research and collection can reveal** the existence of, and sometimes details about, classified or sensitive information or undertakings.
- Purchasing documents, searching an Internet site, or asking questions at public events are examples of detectable techniques that could provide indicators of US plans and operations."
- Determine what level of contact with open sources and which collection techniques might provide indicators that an enemy could piece together in time to affect US military operations.
- In OSINT operations, countermeasures range from limiting the frequency or duration of contact with a source to prohibiting all contact with a source."

Source: FMI 2-22.9

LESSON 1

8/17/2012 9

## OPSEC is Applicable to Any Situation

- Planning and forecasts
  - Special events
  - Disaster preparedness
- At home and on vacation
- Special Training Exercises
- Open Source Searching
- Contracts/Bidding Processes
- Internet Activities
- Personal computing and communication devices

LESSON 1

8/17/2012 10

## What Does This Mean Exactly?

- Be responsible
- Follow rules of your company
- Use common sense rules
- Use an anti-virus software
- Don't say ok, ok, ok, when you install new apps
- Be aware that other people are watching and following your footprints on the Internet

LESSON 1

8/17/2012 11

## Communication Channels

- Email
- Web
- Chat rooms
- Social media and networks
- Bulletin boards
- Internet Relay Chat (IRC); Instant Messaging (IM)

DO NOT SEND ANY proprietary, confidential, sensitive, or classified information via UNSECURE communication channels.

LESSON 1

8/17/2012 12

## Communication Devices

- Personal computer
- Notebook
- Mobile device
  - Cell phone
  - Smart phone
- Telephone
- Fax machine
- Radio

LESSON 1

8/17/2012 13

## Internet Postings

- Guidelines prohibiting the posting of sensitive information
- Don't give any unnecessary information
- Adversary can twist information – we can be our own worst enemy
- What have others posted?
- Posted information is in the public domain FOREVER
  - Forever in search engine caches, copied to another website, and in the Internet archive

LESSON 1

8/17/2012 14

## Persona, your Footprint

Russ Haynal's site:

http://navigators.com/opensource.html

and

Security and Privacy Issues for Internet Users Persona:

http://navigators.com/persona.html

LESSON 1

8/17/2012 15

## Change your Profile

- Adjust security settings and browser preferences
- Change time zone setting
- Change OS language settings
- Use different browsers
- Country or region of origin

LESSON 1

8/17/2012 16

## Browser Issues

- Browser type
- IP address
- Date and time setting
- Number of sites visited today
- Sites history
- Computer name
- Page referred from
- Cookies
- Email address
- Clipboard contents

LESSON 1

8/17/2012 17

## Public Anonymous Proxies

- Organizational restrictions
- You are not anonymous to the proxy provider
- Identified as an anonymized user
- Beware of false sense of security

LESSON 1

8/17/2012 18

## Public Anonymous Proxies - Examples

Anonymizer: www.anonymizer.com

Anonymouse: http://anonymouse.org

Guardster: www.guardster.com

Heeky: www.heeky.com

Hide My Ass: www.hidemyass.com

MegaProxy: www.megaproxy.com/freesurf

My-proxy: www.my-proxy.com

Online Anonymous Proxy: http://zend2.com/

Privoxy: http://sourceforge.net/projects/ijbswa/files/

Tor: www.torproject.org

Try Catch Me: www.trycatchme.com

250+ Working Proxies: http://www.econsultant.com/proxylist/index.html

LESSON 1

8/17/2012 19

## Searching Guidelines

- Adhere to the security mandates of your organization
- Don't bring attention to you, your organization, or your operations
- Conduct research without disclosing your identity or mission
- Keep personal details off of the Internet
- Try to look like everybody else
- Try to avoid patterns
- Discretion and anonymity, not necessarily deception
- Use different email addresses for each website and activity
- Disable anything that records your activity
- Be aware of what your browser is disclosing about you
- Do not automatically open attachments
- Use removable storage media
- Properly dispose of printed and electronic media

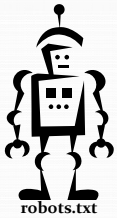
LESSON 1

20

## Sensitive Data

How does it end up in search engine databases?

- Misconfigured servers / incorrect or missing robots.txt file
- Software vulnerabilities
- Human error / ignorance




LESSON 1

8/17/2012 21

## Simple Things to Prevent Problems

- Hover over links and look in the bottom left corner before clicking on URLS that you are uncertain about
- Use common sense to avoid phishing and spam mail
- Watch your downloads—some programs include adware that will report your surfing habits which may result in spam
- Use the INCOGNITO mode of Google Chrome to check out uncertain URLs
- Guard your private information
- Use VPN in public spaces—Panera, Starbucks, hotels
- Use caution when using social media
- Know what https means
- Create long memorable passwords

LESSON 1

8/17/2012 22

## Simple Things to Prevent Problems

- Be careful with email attachments
- Consult with your IT Department for spam filters, anti-virus software, etc.
- Set-up mobile phone passwords
- Don't leave your password on a post-it note
- Many browsers and search engines have auto-complete features—don't enable
- Monitor your online reputation
- Beware of apps that you add to your mobile phone
- Log out of search engines
- Lock your computer when you walk away

LESSON 1

8/17/2012 23

## Computer Security Guidelines

- ✓ Lock your PC before you step away
- ✓ Utilize hardware and software safeguards
- ✓ Examine options and settings for each application to enable security
- ✓ Avoid or disable HTTP-Referrer variable
- ✓ Clear History files and private data after each session
- ✓ Clear Temp files, set Temp space to 1 MB
- ✓ Turn off "Allow paste operations via script" / "Allow Programmatic Clipboard Access"
- ✓ Anti-virus (update regularly)
- ✓ Anti-spyware (update regularly)
- ✓ Back up regularly
- ✓ Firewall (update and secure)
- ✓ Keep your OS and software patched and updated
- ✓ Disable email scripting
- ✓ Don't use administrator logon
- ✓ Don't open unknown attachments
- ✓ Use strong passwords
- ✓ Password protect files
- ✓ Open files in a different viewer
- ✓ Utilize software encryption features

LESSON 1

8/17/2012 24

## Helpful Information

**Cybersecurity**

- Department of Homeland Security. Stop.Think.Connect: www.dhs.gov/files/events/stop-think-connect.shtm
- Federal Trade Commission. Consumer Protection. Protecting America's Consumers: www.ftc.gov/bcp/menus/consumer/tech.shtm
- Infosec Island: infosecisland.com
- United States Computer Emergency Readiness: www.uscert.gov

LESSON 1

8/17/2012 25

## Summary

- Used to increase safety and security
- Risk assessment tool
- Examine day-to-day activities from an adversary's point of view
- Helps you understand what an adversary can learn about your organization from your activities
- It is a mindset
- Applicable to all daily activities

LESSON 1

8/17/2012 26